

What is claimed is:

- Self A7*
1. A method for protecting a data file on a computer system, comprising the steps of:  
5 encrypting the data file using a private key to create an encrypted data file;  
generating a new key;  
10 updating the encrypted data file with the new key to create an updated encrypted  
data file;  
replacing the encrypted data file with the updated encrypted data file; and  
replacing the private key with the new key.
- 15 2. The method of claim 1, further comprising the step of repeating the updating step  
and the two replacing steps on a periodic basis.
- 20 3. The method of claim 1, further comprising the step of decrypting the encrypted  
data file with the private key, wherein the private key has been replaced by the new key,  
and wherein the encrypted data file has been replaced by the updated encrypted data file.
- 25 4. A processor-driven system adapted to protect a data file, the system comprising:  
a processor; and  
a memory coupled to the processor for storing the data file;  
wherein the processor is programmed to perform the steps of:  
encrypting the data file using a private key to create an encrypted data file;  
generating a new key;  
updating the encrypted data file with the new key to create an updated encrypted  
data file;  
replacing the encrypted data file with the updated encrypted data file; and  
replacing the private key with the new key.
- 30 5. The processor-driven system of claim 4, further comprising a communication  
interface.

6. The processor-driven system of claim 4, wherein the processor and the memory are included within a portable device.

7. The processor-driven system of claim 4, wherein the processor and the memory are included within a smart card.

5

A  
B  
C  
D